SANGFOR MDR

Managed Detection & Response

Intelligent Cybersecurity Operations — 24/7 Threat Detection, Investigation & Response

90%	85%	24/7
Faster Detection	Faster Response	Expert Coverage

What is Sangfor MDR?

Sangfor Managed Detection and Response (MDR) is a fully managed cybersecurity service that delivers continuous 24/7 threat monitoring, AI-powered detection, expert investigation, and hands-on incident response. Unlike traditional MSSPs that simply forward alerts, Sangfor MDR actively hunts threats, investigates incidents, and contains attackers — reducing breach impact before significant damage occurs.

Powered by Sangfor's Neural-X AI engine and backed by a global Security Operations Center (SOC), MDR integrates endpoint, network, cloud, and identity telemetry into a unified threat operations platform.

Core Architecture

Data Collection & Visibility

- Endpoint Detection & Response (EDR) — process events, file activity, registry changes
- Network Detection & Response (NDR) — east-west and north-south traffic analysis
- SIEM log ingestion — firewalls, VPNs, cloud platforms, identity providers
- Cloud workload coverage — AWS, Azure, Alibaba Cloud, containers

AI-Powered Detection (Neural-X)

- Machine learning models trained on billions of global threat indicators
- User & Entity Behavior Analytics (UEBA) for insider threat detection
- Real-time MITRE ATT&CK framework correlation and threat intelligence enrichment
- Deception technology — honeypots and honey tokens for lateral movement detection

24/7 Expert SOC

Sangfor's global SOC operates across multiple time zones with Tier 1–3 analysts, dedicated threat hunters, and an incident response team providing remote or on-site containment, eradication, and recovery support.

SOAR — Automated Response

- Automated playbooks for ransomware, phishing, credential stuffing, and more
- One-click endpoint isolation, IP blocking, and file quarantine
- Ransomware rollback — restore encrypted files within minutes

Sangfor MDR vs. Alternatives

Feature	Trad. SOC	Std. MDR	Sangfor MDR
24/7 Monitoring	✓	✓	✓
AI Threat Detection	Basic	✓	✓
Active Threat Hunting	—	Limited	✓
SOAR Automation	—	Limited	✓
Ransomware Rollback	—	—	✓
Compliance Reporting	✓	✓	✓

© 2026 Spollex Distribution | www.spollex.com

Key Capabilities

Threat Hunting
Proactive, hypothesis-driven hunting uncovers threats that evade automated detection — searching endpoints, logs, and network traffic for hidden adversaries.

Ransomware Defense
Multi-layered protection: pre-execution AI blocking, real-time encryption interruption, and post-event file rollback to minimize downtime.

Vulnerability Management
Continuous asset exposure monitoring, CVE correlation, and prioritized remediation guidance to close gaps before attackers exploit them.

Phishing & Email Security
Email gateway integration with URL detonation in sandboxed environments and rapid removal of malicious messages from affected mailboxes.

Compliance Reporting
Automated reports aligned to ISO 27001, GDPR, NIST CSF, PCI-DSS, and MAS TRM for seamless audits and board-level visibility.

Cloud & OT Coverage
Extends protection to cloud workloads, containers, and OT/ICS environments using passive monitoring that does not disrupt industrial operations.

Deployment Models

Cloud-Native	On-Premise	Hybrid
Full cloud delivery. Secure telemetry transmission with data residency options.	Analytics engine and data within your own infrastructure — ideal for regulated industries.	On-premise collection with cloud analytics — balancing sovereignty, scale, and speed.

Business Value & ROI

Sangfor MDR delivers enterprise-grade security operations at 40–60% of the cost of an in-house SOC, eliminating the challenge of recruiting scarce cybersecurity talent. Beyond cost savings, MDR dramatically limits the blast radius of incidents — reducing dwell time from months to minutes and preventing the multi-million dollar losses associated with undetected breaches.

- Up to 90% reduction in Mean Time to Detect (MTTD)
- Up to 85% reduction in Mean Time to Respond (MTTR)
- Measurable security posture improvement within 6–12 months
- Supports compliance with ISO 27001, GDPR, NIST CSF, PCI-DSS, MAS TRM

Get Started with Sangfor MDR
Contact us to learn more
info@spollex.com
www.spollex.com